Paper reference 20158K
Pearson BTEC
Level 3 Nationals Diploma, Extended Diploma

INFORMATION TECHNOLOGY

UNIT 11: CYBER SECURITY AND INCIDENT MANAGEMENT

(Part A)

Supervised hours: 5 hours plus your additional time allowance

X64265A

Pearson

YOU MUST HAVE:

Risk_Assessment.rtf,
Security_Plan.rtf,

YOU WILL BE GIVEN

- **A separate Data Book.**

INSTRUCTIONS

- **Part A and Part B contain material for the completion of the set tasks under supervised conditions.**
- **There are 43 marks for Part A and 37 marks for Part B, giving a total mark for the set tasks of 80.**
- **Part A and Part B are specific to each series and this material must be issued only to learners who have been entered to take the tasks in the specified series.**
- **This booklet should be kept securely until the start of the 5 – hour (plus your additional time allowance), Part A supervised assessment period.**
- **Part A will need to have been completed and kept securely before starting Part B.**

(continued on the next page)

- **Both parts will need to be completed during the 3 – week period timetabled by Pearson.**
- **Part A and Part B tasks must be submitted together for each learner.**
- **This booklet should not be returned to Pearson.**
- **Answer ALL activities.**

INFORMATION

- **The total mark for this Part is 43.**

INSTRUCTIONS TO INVIGILATORS is on the next page

INSTRUCTIONS TO INVIGILATORS

This paper must be read in conjunction with the unit information in the specification and the BTEC Nationals Instructions for Conducting External Assessments (ICEA) document. See the Pearson website for details.

Refer carefully to the instructions in this task booklet and the BTEC Nationals Instructions for Conducting External Assessments (ICEA) document to ensure that the assessment is supervised correctly.

Part A and Part B set tasks should be completed during the period of 3 weeks timetabled by Pearson. Part A must be completed before starting Part B.

The 5 – hour Part A set task must be carried out under supervised conditions.

The set task can be undertaken in more than one supervised session.

(continued on the next page)

Electronic templates for activities 1 and 2 are available on the website for centres to download for learner use.

Learners must complete this task on a computer using the templates provided and appropriate software. All work must be saved as PDF documents for submission.

Invigilators may clarify the wording that appears in this task but cannot provide any guidance in completion of the task.

Invigilators should note that they are responsible for maintaining security and for reporting issues to Pearson.

(continued on the next page)

MAINTAINING SECURITY

- Learners must not bring anything into the supervised environment or take anything out.
- Centres are responsible for putting in place appropriate checks to ensure that only permitted material is introduced into the supervised environment.
- Internet access is not permitted.
- Learner's work must be regularly backed up. Learners should save their work to their folder using the naming instructions indicated in each activity.
- During any permitted break, and at the end of the session, materials must be kept securely and no items removed from the supervised environment.
- Learners can only access their work under supervision.
- User areas must only be accessible to the individual learners and to named members of staff.

(continued on the next page)

- **Any materials being used by learners must be collected in at the end of each session, stored securely and handed back at the beginning of the next session.**
- **Following completion of Part A of the set task, all materials must be retained securely for submission to Pearson.**
- **Part A materials must not be accessed during the completion of Part B.**

(continued on the next page)

OUTCOMES FOR SUBMISSION

Each learner must create a folder to submit their work. Each folder should be named according to this naming convention:

[Centre #]_[Registration number #]_ [surname]_[first letter of first name]_U11A

Example: Joshua Smith with registration number F180542 at centre 12345 would have a folder titled

12345_F180542_Smith_J_U11A

Each learner will need to submit 3 PDF documents within their folder, using the file names listed.

ACTIVITY 1:

activity1_riskassessment_[Registration number #]_[surname]_[first letter of first name]

ACTIVITY 2:

activity2_securityplan_[Registration number #]_[surname]_[first letter of first name]

(continued on the next page)

ACTIVITY 3:

activity3_managementreport_[Registration number #]_[surname]_[first letter of first name]

An authentication sheet must be completed by each learner and submitted with the final outcomes.

The work should be submitted no later than 2 February 2022.

INSTRUCTIONS FOR LEARNERS is on the next page

INSTRUCTIONS FOR LEARNERS

Read the set task brief carefully.

Plan your time carefully to allow for the preparation and completion of all the activities.

Your centre will advise you of the timing for the supervised period. It is likely that you will be given more than one timetabled session to complete these tasks.

Internet access is not allowed.

You will complete this set task under supervision and your work will be kept securely at all times.

You must work independently throughout the supervised assessment period and must not share your work with other learners.

Your invigilator may clarify the wording that appears in this task but cannot provide any guidance in completion of the task.

(continued on the next page)

You should only consider threats, vulnerabilities, risks and security protection measures that are implied and / or specified in the set task brief.

Part A materials must not be accessed during the completion of Part B.

(continued on the next page)

OUTCOMES FOR SUBMISSION

You must create a folder to submit your work.
The folder should be named according to this naming convention:

[Centre #]_[Registration number #]_ [surname]_[first letter of first name]_U11A

Example: Joshua Smith with registration number F180542 at centre 12345 would have a folder titled

12345_F180542_Smith_J_U11A

You will need to submit 3 PDF documents within your folder, using the file names listed.

ACTIVITY 1:
activity1_riskassessment_[Registration number #]_[surname]_[first letter of first name]

ACTIVITY 2:
activity2_securityplan_[Registration number #]_[surname]_[first letter of first name]

(continued on the next page)

ACTIVITY 3:

activity3_managementreport_[Registration number #]_[surname]_[first letter of first name]

You must complete an authentication sheet before you hand your work into your invigilator.

SET TASK BRIEF is on the next page

SET TASK BRIEF

Hotela Ĉeno

Reganta Virino is the Chief Executive of Hotela Ĉeno (HC), a hotel chain on the island of Varma Loko. The hotels are rated as four star and HC gets most of its business from the tourist trade. It gets block bookings for package tours by international holiday companies and individual bookings by independent travellers.

Reganta is planning a new hotel near Varma Loko Airport. It will cater for short stay travellers and flight crew. Reganta knows that these guests will have different needs from guests staying at other HC hotels.

(continued on the next page)

SET TASK BRIEF continued

Look at Figure 1 and Figure 2 in the separate Data Book. Figure 1 and Figure 2 show a provisional plan of the new hotel. The hotel will have four floors. Details have not been finalised but Reganta's idea is to:

- **use the ground floor for:**
  - **reception area**
  - **a conference suite and meeting rooms**
  - **an IT centre**
  - **a restaurant and bar**
  - **hotel services such as kitchens, storage, offices, and utilities.**
- **use the top three floors for bedrooms, each floor having:**
  - **40 bedrooms with outside views**
  - **30 bedrooms with inside views.**
- **have an outdoor swimming pool**
- **have an area of gardens with a bar-cafe**
- **use one side of the hotel grounds for parking**
- **use the other side for leisure facilities such as tennis courts, gym equipment, and a children's play area.**

(continued on the next page)

SET TASK BRIEF continued

Reganta wants the hotel to compete for customers with other hotels near the airport. She plans to offer services, which she believes will attract customers. These include:

- **free public WiFi in public areas such as the restaurant and gardens**
- **free guest WiFi, with a higher available bandwidth, in the bedrooms**
- **a direct feed from the airport to Arrival and Departure displays in public areas**
- **a regular minibus service between the hotel and the airport, with a moving map display in reception. The display will show the position of the minibuses and estimated arrival times**
- **a facility for guests to book rental cars, taxis, tours, guides, and other tourist related services**
- **a facility for guests to check in for flights and print boarding cards, e–tickets, flight details, etc.**

(continued on the next page)

SET TASK BRIEF continued

Reganta has many years of management experience in the hotel business but regards herself as an IT user rather than an IT specialist. She uses HC's IT and administrative staff for anything more than basic computing tasks.

Reganta will use HC's staff to create the IT system but thinks it would be a good idea to have someone who is not employed by the hotel chain to advise on the system. She has hired you to advise on cyber security and incident management.

(continued on the next page)

SET TASK BRIEF continued

DEVELOPMENT PLAN

At a meeting with Reganta you establish that:

1. **Network connectivity should conform to the outline network diagram. Look at Figure 3 in the separate Data Book. It shows the network connectivity.**
2. **WiFi connectivity should be available as widely as possible.**
3. **Reganta is concerned about the vulnerability of WiFi links.**
4. **The main system must control Internet of Things (IoT) systems such as lighting, air conditioning, public address, and environmental monitoring.**
5. **Guests must not be able to access any of the hotel's IoT systems.**
6. **Reganta requires high availability with at least 99% uptime on the system.**
7. **Public / guest interfaces to the system must be available in many different languages.**

Part A SET TASK is on the next page

Part A SET TASK

You must complete ALL activities in the set task.

Read the set task brief carefully before you begin and note that reading time is included in the overall assessment time.

Reganta has hired you to advise on cyber security and incident management.

You should only consider threats, vulnerabilities, risks and protection measures that are implied and / or specified in the set task brief.

Design cyber security protection measures for the given computer network.

ACTIVITY 1 is on the next page

ACTIVITY 1: RISK ASSESSMENT OF THE NETWORKED SYSTEM – You are advised to spend 1 hour and 30 minutes (plus your additional time allowance) on this activity.

Duplicate (copy and paste) and complete the risk assessment using the template given for each threat.

Produce a cyber security risk assessment using the template Risk_Assessment.rtf

Save your completed risk assessment as a PDF in your folder for submission as

activity1_riskassessment_[Registration number #]_[surname]_[first letter of first name]

(Total for Activity 1 = 8 marks)

ACTIVITY 2: CYBER SECURITY PLAN FOR THE NETWORKED SYSTEM – You are advised to spend 2 hours and 30 minutes (plus your additional time allowance) on this activity.

Using the template Security_Plan.rtf produce a cyber security plan for the computer network using the results of the risk assessment.

For each protection measure, you must consider:

(a) threat(s) addressed by the protection measure

(b) action(s) to be taken

(c) reasons for the action(s)

(d) overview of constraints – technical and financial

(e) overview of legal responsibilities

(f) overview of usability of the system

(g) outline cost – benefit

(h) test plan.

(continued on the next page)

ACTIVITY 2 continued

Duplicate (copy and paste) and complete the cyber security plan using the template given for each protection measure, as appropriate.

Save your completed security plan as a PDF in your folder for submission as

activity2_securityplan_[Registration number #]_[surname]_[first letter of first name]

(Total for Activity 2 = 20 marks)

ACTIVITY 3: MANAGEMENT REPORT JUSTIFYING THE SOLUTION – You are advised to spend 1 hour (plus your additional time allowance) on this activity.

Produce a management report, justifying how the proposed cyber security plan will meet the security requirements of the set task brief.

The report should include:

- **an assessment of the appropriateness of your protection measures**
- **a consideration of alternative protection measures that could be used**
- **a rationale for choosing your protection measures over the alternatives.**

(continued on the next page)

ACTIVITY 3 continued

Save your completed management report as a PDF in your folder for submission as

activity3_managementreport_[Registration number #]_[surname]_[first letter of first name]

(Total for Activity 3 = 12 marks)

TOTAL FOR TECHNICAL LANGUAGE IN PART A = 3 MARKS

TOTAL FOR PART A = 43 MARKS

END OF PAPER
